Abstract

The presented methods form the basis of a forward-secure signature scheme that is provably secure. Moreover, the presented methods form also the basis of a fine-grained forward-secure signature scheme that is secure and efficient. The scheme allows to react immediately on hacker break-ins such that signatures from the past still remain valid without re-issuing them and future signature values based on an exposed key can be identified accordingly. In general, each prepared signature carries an ascending index such that once an index is used, no lower index can be used to sign. Then, whenever an adversary breaks in, an honest signer can just announce the current index, e.g., by signing some special message with respect to the current index, as part of the revocation message for the current time period. It is then understood that all signatures made in prior time periods as well as all signatures make in the revoked period up to the announced index are valid, i.e., non-reputable.

[Fig. 3]